Política de Seguridad Física

Forestal Collicura Limitada

Información del documento

Versión	Fecha de Creación		Descripción
1.0	28-07-2023		Creación y primera versión del documento.

(*) La última versión sustituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los efectos.

Tabla de contenido

1. *Introducción*

Con el objeto de tener una estructura de seguridad física de acuerdo con la realidad actual y para proteger la información y los principales activos digitales y físicos, que **FORESTAL COLLICURA LIMITADA** administra ya sea por parte del objetivo que fue creada o de los terceros que encargan sus datos, debe existir un resguardar al acceso físico a todas las instalaciones, rack o salas donde equipamiento de infraestructura TI funcione.

En esta política se definen las medidas necesarias que debemos cumplir para mantener la confidencialidad de la información en relación a la seguridad física de los activos de **FORESTAL COLLICURA LIMITADA**.

2. *Objetivo*

Controlar y gestionar el acceso físico, determinar las áreas seguras con sus perímetros de seguridad física, sus controles físicos de entrada, seguridad de las oficinas, despachos y recursos, junto a la protección contra las amenazas externas y ambientales, áreas de trabajo seguras y áreas de carga y descarga.

Las medidas de protección deben ser consistentes con el nivel de clasificación de los activos y el valor de la información procesada y almacenada en las instalaciones.

3. *Alcance*

Esta política se aplica a todo el personal con contrato parcial, tiempo completo, a honorarios, y estudiante en **FORESTAL COLLICURA LIMITADA** y también al personal

externo que preste o prestare servicios, remunerados o no a **FORESTAL COLLICURA LIMITADA**. Para esta última condición es vital que los contratistas tenga conocimiento de esta política por parte de los encargados de realizar los contratos con ellos o por medio de las áreas de Ciberseguridad.

4. Definiciones

Confidencialidad: Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.

Áreas seguras: Áreas donde se procesa o se almacena información sensible. Por ejemplo Data Centers, sala de servidores, rack de comunicaciones.

Biometría: Tecnología de identificación basada en el reconocimiento de una característica física e intransferible de las personas, como, por ejemplo, la huella digital o el reconocimiento facial.

5. Política

5.1 Áreas seguras

5.1.1 Perímetro de seguridad física

Se deben considerar e implementar, los siguientes lineamientos para los perímetros de seguridad física:

- Los perímetros de seguridad deben estar claramente definidos, y la situación y robustez de cada perímetro debe depender de los requisitos de seguridad de los activos dentro del perímetro.

- El ingreso a las áreas seguras de **FORESTAL COLLICURA LIMITADA** deben estar adecuadamente protegidas contra los accesos no autorizados a través de mecanismos de control, por ejemplo: tarjetas de control de acceso, código PIN, biometría.
- Se debe contar con sistemas de detección de intrusión adecuados conforme a las normas nacionales e internacionales y ser probados periódicamente para dar cobertura a todas las puertas externas y ventanas accesibles; las áreas no ocupadas deben estar dotadas de un sistema de alarma en todo momento.
- Las zonas anteriores deben estar debidamente señalizadas con su grado de confidencialidad.
- Los departamentos que administren estas unidades o zonas deben informar al área de Ciberseguridad en forma periódica los cambios de estructura que estas dependencias sufran o sus contingencias en relación con los accesos a estos lugares.
- Los departamentos que administren estas unidades además deben informar al área de Ciberseguridad el listado de las personas que trabajan en estos lugares para gestionar sus anexos de contratos de confidencialidad con RR.HH. Así también se debe informar cualquier cambio de personal o de autorizaciones.
- Todos los controles de acceso habilitados deben tener auditorías mensuales y los informes deben ser enviados directamente a la autoridad más alta de **FORESTAL COLLICURA LIMITADA.**
- Así también las áreas de Ciberseguridad podrán auditar en forma aleatoria los accesos y los permisos otorgados.
- Para el control de los accesos debe haber un sistema que registre las autorizaciones como excepción en caso de mantenciones o habilitación de nuevos servicios.
- Nadie puede acceder a las salas de datos o rack de comunicaciones, o dependencias consideradas como confidenciales fuera del horario de oficina sin la autorización del área de Ciberseguridad.

5.1.2 Controles físicos de entrada

Se deben considerar las siguientes directrices para asegurar que únicamente se permite el acceso al personal autorizado a las áreas seguras:

- Se debe registrar la fecha y la hora de entrada y salida de los visitantes. Todos los visitantes deben ser supervisados a menos que su acceso haya sido previamente aprobado; únicamente se debe conceder el acceso para propósitos específicos y autorizados, y junto con el acceso se deben proporcionar las instrucciones de los requisitos de seguridad del área y los procedimientos de emergencia. La identidad de los visitantes debe autenticarse mediante los medios adecuados.
- El acceso a las áreas donde se procesa o se almacena información sensible debe estar controlado y restringido únicamente a personal autorizado; se deben utilizar controles de autenticación para autorizar y validar todos los accesos, por ejemplo: mecanismo de doble factor de autenticación como tarjetas de control de acceso con número de identificación personal secreto (PIN).
- Debe mantenerse y monitorizarse de manera segura un libro físico o digital con el registro de todos los accesos a las áreas seguras.
- Debe requerirse a todos los colaboradores, contratistas y terceros y a todos los visitantes, llevar una identificación visible dentro de las áreas seguras.
- Para el personal proveniente de terceros que prestan servicios de apoyo, se debe proporcionar acceso restringido a las áreas seguras o a los recursos de tratamiento de la información sensible únicamente cuando sea requerido; este acceso debe estar autorizado y controlado.
- Los derechos de acceso a las áreas seguras deben ser revisados y actualizados regularmente, y revocados cuando sea necesario.

- La responsabilidad de las áreas seguras siempre será del dueño del activo, jefe de Departamento o Ejecutivo que tenga la responsabilidad de la zona segura.
- Cualquier transgresión de estas normas se considera un incidente crítico dentro de las normas establecidas en la ISO 27001.

5.2 Seguridad de los equipos

5.2.1 Protección de equipos

Se deben considerar las siguientes directrices para proteger los equipos:

- Se deben adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales como, por ejemplo, robo, fuego, explosivos, humo, agua (o fallo de suministro de agua), polvo, vibración, agentes químicos, interferencias en el suministro eléctrico, interferencias en las comunicaciones, radiaciones electromagnéticas y vandalismo.
- Se deben controlar las condiciones ambientales, tales como la temperatura y la humedad, que puedan afectar negativamente al funcionamiento de los equipos de tratamiento de información.

5.2.2 Mantenimiento de los equipos

Se deben considerar las siguientes directrices para el mantenimiento de los equipos:

- Los equipos deben mantenerse de acuerdo con las recomendaciones de intervalos de servicio y especificaciones del proveedor.
- Solo el personal de mantenimiento debidamente autorizado debe realizar la reparación y el servicio de los equipos.

- Se deben mantener registros de todos los fallos, reales o sospechados, así como de todo el mantenimiento preventivo y correctivo.

5.2.3 Puesto de trabajo despejado, pantalla limpia y seguridad física de los equipos

- La información considerada sensible o crítica en formato físico debería estar guardada bajo llave cuando no se necesite, especialmente cuando la oficina está vacía.
- Los encargados de la información ya sea física o digital son los responsables de asegurar que esta información esté debidamente resguardada y ante cualquier duda de procedimiento o estructura deben consultar al área de Ciberseguridad.
- Todos los equipos portátiles y fijos de **FORESTAL COLLICURA LIMITADA** deben tener la posibilidad de quedar con un candado de seguridad y en caso de poseer discos de estado sólido es obligatorio que estos estén cifrados.
- Los equipos computacionales deben quedar apagados o protegidos mediante un mecanismo de bloqueo de pantalla protegido con contraseña cuando estos se encuentren desatendidos.

5.2.4 Auditorias y control

- El área de Ciberseguridad podrá realizar auditorías de seguridad interna de acuerdo con la clasificación de las áreas.
- La información de las auditorías internas es reservada y podrá ser realizada a las instalaciones y a las personas.

6. Responsabilidades

***Personal de* FORESTAL COLLICURA LIMITADA**: Tiene la responsabilidad de cumplir con lo formalizado en este documento y aplicarlo en su entorno laboral.

Área de Ciberseguridad: Es el principal responsable en la definición de los criterios de seguridad de la información en **FORESTAL COLLICURA LIMITADA**, para lo cual deberá analizar periódicamente el nivel de riesgo existente, proponiendo soluciones. Una vez autorizada la implementación de las medidas, deberá coordinar con quienes corresponda su materialización oportuna y correcta.

***Ejecutivos o Altos Cargos de* FORESTAL COLLICURA LIMITADA**: Son responsables de hacer cumplir estas indicaciones en todas sus áreas de responsabilidad y sensibilizar a sus subordinados del cumplimiento de esta política

7. Documentación de referencia

El presente documento constituye una política específica destinada a la seguridad física sigue los lineamientos del "Código de prácticas para los controles de seguridad de la información ISO/IEC 27002". Para los procedimientos específicos relacionados con este tema, todos deben estar alineados con esta política.